In The United States Patent and Trademark Office

In re Application of: Rump, et al. **Docket No.:** SCHO0113

Serial No. : 09/913,695 **Art Unit:** 2131

Filed: August 2, 2002 **Examiner:** Henning, M.

Title: METHOD AND DEVICE FOR GENERATING AN ENCRYPTED USER DATA STREAM AND METHOD AND DEVICE FOR PLAYING BACK AN ENCRYPTED USER DATA STREAM

May 11, 2006

MAIL STOP - AMENDMENT
Commissioner for Patents
PO BOX 1450
Alexandria VA 22313-1450

AMENDMENT UNDER 37 CFR § 1.111

Sir:

Applicant provides this Amendment in responsive to the Office Action, dated February 23, 2006, in the above-identified patent application. A listing of the claim is provided starting at sheet #2 of this paper. Remarks begin at sheet #6 of this paper.

The Commissioner is authorized to charge any fees that may be due and to credit any overpayments to Deposit Account 07-1445, Glenn Patent Group.

CLAIMS

1. (currently amended) A method for generating an encrypted user data stream, which has a start block and a user data block, comprising the following steps:

generating the start block; and

generating the user data block, which follows the start block, by means of the following substeps:

using a first part of the user data ~~to be encrypted~~ as a start section for the user data block, the start section ~~being~~ remaining unencrypted;

encrypting a second part of user data ~~to be encrypted~~ which follow the first part of the user data to obtain encrypted data; and

appending the encrypted user data to the unencrypted start section.

2. (original) A method according to claim 1, wherein the step of generating the start block includes the following substep:

entering the length of the start section in the start block.

3. (original) A method according to claim 1, wherein the second part does not comprise all the user data to be encrypted and wherein the step of generating the user data block includes the following substep:

appending a third part of user data to be encrypted, which follow the second part, to the encrypted user data of the second part, the user data of the third part being unencrypted.

4. (currently amended) A method according to claim 1, wherein the step of generating the start block includes the following substep:

entering the length of the encrypted ~~multimedia~~ user data, ~~which correspond to the user data~~ of the second part which are to be encrypted, in the start block.

5. (original) A method according to claim 3, wherein the step of generating the start block also includes the following substep:

entering the sum of the length of the encrypted user data, which correspond to the second part, and the length of the third part of the unencrypted user data in the start block.

6. (original) A method for playing back an encrypted multimedia data stream, which has a start block and a user data block, where a start section of the user data block, which follows the start block, contains unencrypted user data and where a further section of the user data block contains encrypted user data, where the start block contains information which is needed to play back the start section of the user data block and where the start block contains information which is not needed to play back the unencrypted start section of the user data block, comprising the following steps:

processing the information of the start block which is needed to play back the start section of the user data block; and

playing back the unencrypted start section of the user data block.

7. (original) A method according to claim 6, which also includes the following steps:

processing the information of the start block which is not needed to play back the unencrypted start section;

decrypting the further section of the user data block using the processed information of the start block; and

playing back the encrypted user data of the further section of the user data block.

8. (currently amendedl) A method according to claim 7, wherein the step of processing the information of the start block which is not needed to play back the unencrypted start section is performed ~~essentially~~ concurrently with the playing back of the unencrypted start section.

9. (original) A method according to claim 6, wherein the length of the unencrypted start section of the user data block is between 1 and 60 seconds.

10. (original) A method according to claim 6, wherein the user data to be encrypted are coded and wherein the information which is needed for playing back contains an entry specifying the type of coding/decoding method.

11. (original) A method according to claim 1, wherein the user data are audio and/or video data.

12. (currently amended) A device for generating an encrypted user data stream, which has a start block and a user data block, comprising:

a unit for generating the start block; and

a unit for generating the user data block, which follows the start block, with the following features:

a unit for using a first part of the user data ~~to be encrypted~~ as start section for the user data block, the start section ~~being~~ remaining unencrypted;

a unit for encrypting a second part of the user data ~~to be encrypted~~ which follows the first part to obtain encrypted user data; and

a unit for appending the encrypted user data to the unencrypted start section.

13. (currently amended) A device for playing back an encrypted user data stream, which has a start block and a user data block, where a start section of the user data block, which follows the start block, contains unencrypted user data and where a further section of the user data block contains encrypted user data, where the start block contains information which is needed to play back the start section of the user data block and where the start block contains information which is not needed to play back the unencrypted start section of the user data block, comprising:

a unit for processing only the information of the start block which is needed to play back the start section of the user data block; and

a unit for playing back the unencrypted start section of the user data block in response to the unit for processing.

14. (original) A device according to claim 13, which further comprises:

a unit for processing the information of the start block which is not needed to play back the unencrypted start section;

a unit for decrypting the further section of the user data block using the processed information of the start block; and

a unit for playing back the encrypted user data of the further section of the user data block.

15. (currently amended) A device according to claim 14, wherein the unit for processing the information of the start block which is not needed to play back the unencrypted start section is designed to be operated ~~essentially~~ concurrently to the unit for playing back the unencrypted start section.

16. (original) A device according to claim 13, which is implemented as a stereo system, hifi unit, solid state player, a playback unit with a hard disk or CD ROM, or a computer.

17. (original) A device according to claim 12, wherein the user data are audio and/or video data.

18. (new) A method of playing back an encrypted user data stream, which has a start block and a user data block, where a start section of the user data block, which follows the start block, contains unencrypted user data and where a further section of the user data block contains encrypted user data, where the start block contains information which is needed to play back the start section of the user data block and where the start block contains information which is not needed to play back the unencrypted start section of the user data block, comprising:

processing only the information of the start block which is needed to play back the start section of the user data block; and

playing back the unencrypted start section of the user data block in response to the step of processing.

REMARKS

1. Applicant thanks the Examiner for the Examiner's comments which have greatly assisted Applicant in responding.

2. **35 U.S.C. § 112.**

Claims 4, 8 and 15 stand rejected under 35 U.S.C. § 112, 2nd ¶, as being indefinite for failing to particularly point out and distinctly claim the subject matter of the invention. Applicant has amended the claims to eliminate the indefinite language pointed out. Accordingly, the rejection of claims 4, 8 and 15 under 35 U.S.C. § 112 is deemed to be overcome.

3. **35 U.S.C. § 102**

Claims 1-3, 11-12 and 17 stand rejected under 35 U.S.C. § 102(e), as being anticipated by U.S. Patent No. 6,744,894 ("Saito"). Applicant respectfully disagrees.

Saito describes a system to ensure security of data in a computer network system. If one considers Figure 4G of Saito, the first starting portion after the header is encrypted. This is indicated by the separate rectangle around the term "data." These portions are titled "square framed portions," which are encrypted as described at col. 7, lines 61-62. In contrast, claim 1 of the present application explicitly describes a method, wherein the start portion of the user data block following the start block is unencrypted. Contrary thereto, Saito shows, in figure 4G that the first user data block titled "data" following the header is an encrypted data block.

Accordingly, Saito does not anticipate that subject matter of the present inventive as defined in claim 1, because claim 1 says that the start section of the user data block is unencrypted, while all embodiments in Saito explicitly say the start section of the user data block definitely is encrypted. This is evident from Figures 4C, 4D, 4E, 4F, or Fig. 4G of Saito.

In spite of the above, Applicant amends claim 1 to distinguish it from Saito more clearly, by describing that the start section of the user data block remains unencrypted. Therefore, the rejection of claim 1 as being anticipated by Saito is deemed to be overcome. Claim 12 has been amended in similar fashion to claim 1. Accordingly, the

rejections of claims 1 and 12 as being anticipated by Saito are deemed to be overcome. In view of their dependency from allowable base claims, the dependents are also deemed to be allowable without any separate consideration of their merits.

4. **35 U.S.C. § 103·**

Claims 2, 4-6, 10 and 13 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Saito. In view of the foregoing, the present rejections are deemed to be overcome as to claims 2, 4-6 and 10. Applicant respectfully disagrees as to claim 13. The above remarks regarding claims 1 and 12 apply equally to claim 13. Additionally, Saito does not describe that the header includes a part requiring information for playing the first unencrypted start section of the user data block and second information required for decrypting the following encrypted data block. Instead, because the start section of the user data block is encrypted data in all embodiments of Saito, this encrypted data block cannot be played back without encryption, because, the start section of the user data block is unencrypted in the invention, while it is encrypted in Saito. Claim 13 has been amended to more thoroughly describe the above inventive features. Accordingly, the rejection of claim 13 as being unpatentable over Saito is deemed to be overcome.

5. New claim 18 has been added to the Application, which is the parallel method claim for the device of claim 13. Therefore, no new matter is added by way of new claim 18.

CONCLUSION

Based on the foregoing, Applicant considers the Application to be in condition for allowance. Accordingly, reconsideration and prompt allowance of the claims is earnestly requested. Should the Examiner have any questions regarding the Application, he is urged to contact Applicant's attorney at 650-474-8400.

Respectfully Submitted,

Michael A. Glenn
Reg. No. 30,176

Customer No. 22862